Cybersecurity Survey of State Legislators & Staff

AT&T

NATIONAL CYBERSECURITY ALLIANCE

Todd Sander
Vice President, Research
e.Republic Inc.
Tsander@erepublic.com

Report Background

Purpose

The Governing Institute conducted a survey of state elected and appointed officials and their staff to better understand their priorities and knowledge as it relates to cybersecurity.

Key questions included their understanding and knowledge of cybersecurity, primary sources of information about cybersecurity, what cybersecurity threats pose the greatest risk to their state, and barriers to appropriately protect their state from cyberattacks.

The purpose of this survey was to examine current baseline cybersecurity knowledge of state elected and appointed officials in order to identify educational needs regarding this topic.

Methodology

The Governing Institute surveyed a total of 103 respondents – 74 state elected and appointed officials,
and 29 legislative staff members, to better gauge their knowledge of cybersecurity and cybersecurity practices
at the state level.

Responses were gathered from members of our Governing Exchange and members of the National Conference of State Legislatures (NCSL). An online survey was fielded in October and November 2015.

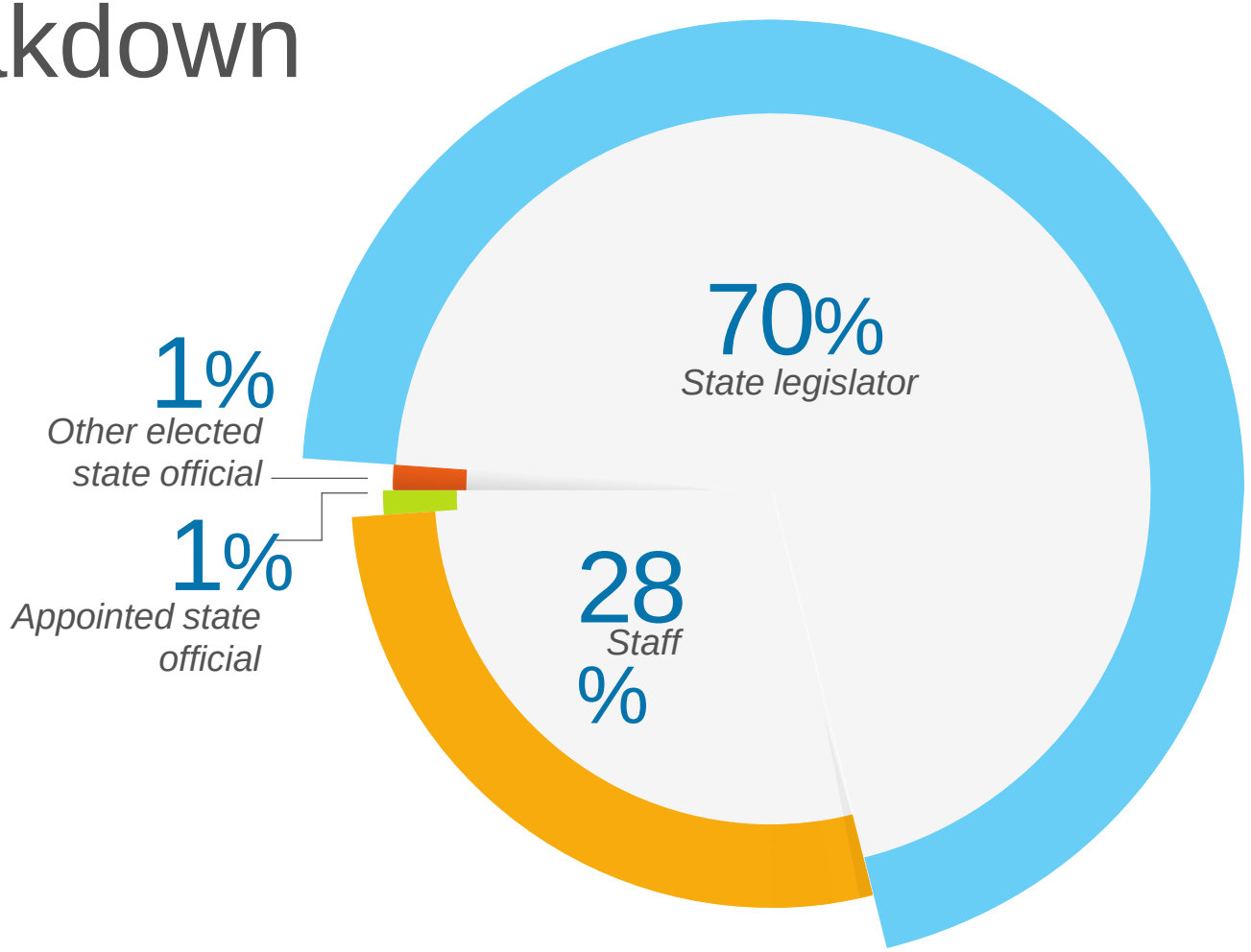
The survey results are reflective of those who subscribe to the Governing Exchange and NCSL.

For the purposes of this survey, cybersecurity was defined to relate specifically to all state networks, state data centers, etc.

Respondent Type Breakdown

Received responses from
74 state elected and appointed officials and 29 staff members

Please select the option that best describes your role/state elected or the appointed official that you report to:



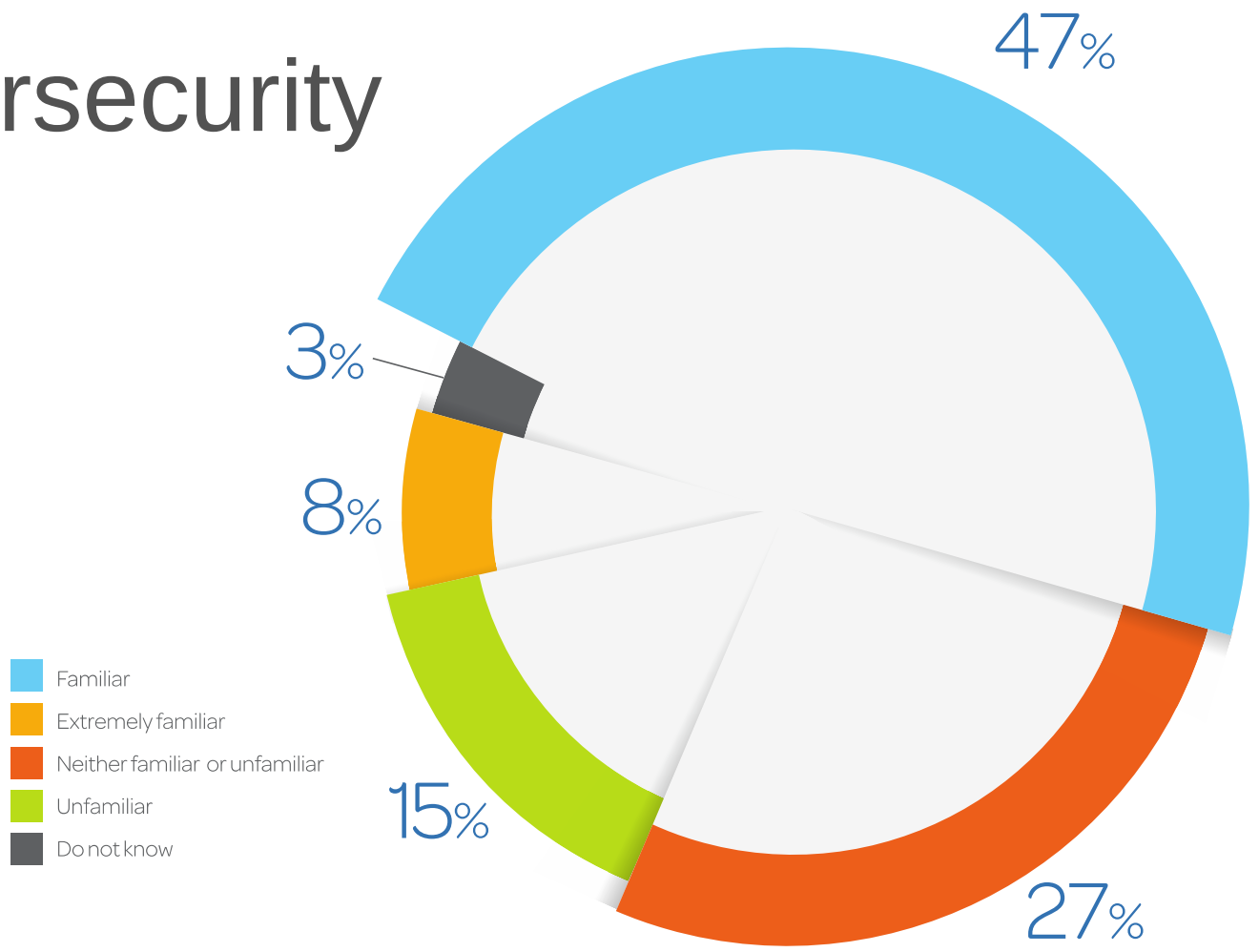
Highlights – Perceptions of Cybersecurity

- Over half of respondents report that they are familiar with cybersecurity
- A majority believe the quality of their state's approach to cybersecurity is on par or average with other states
- A majority agree that cybersecurity is a priority for them
- Two-thirds believe that their state's current level of cyber risk is moderate to high

Familiarity with Cybersecurity

Almost three-quarters of respondents are familiar or extremely familiar with cybersecurity

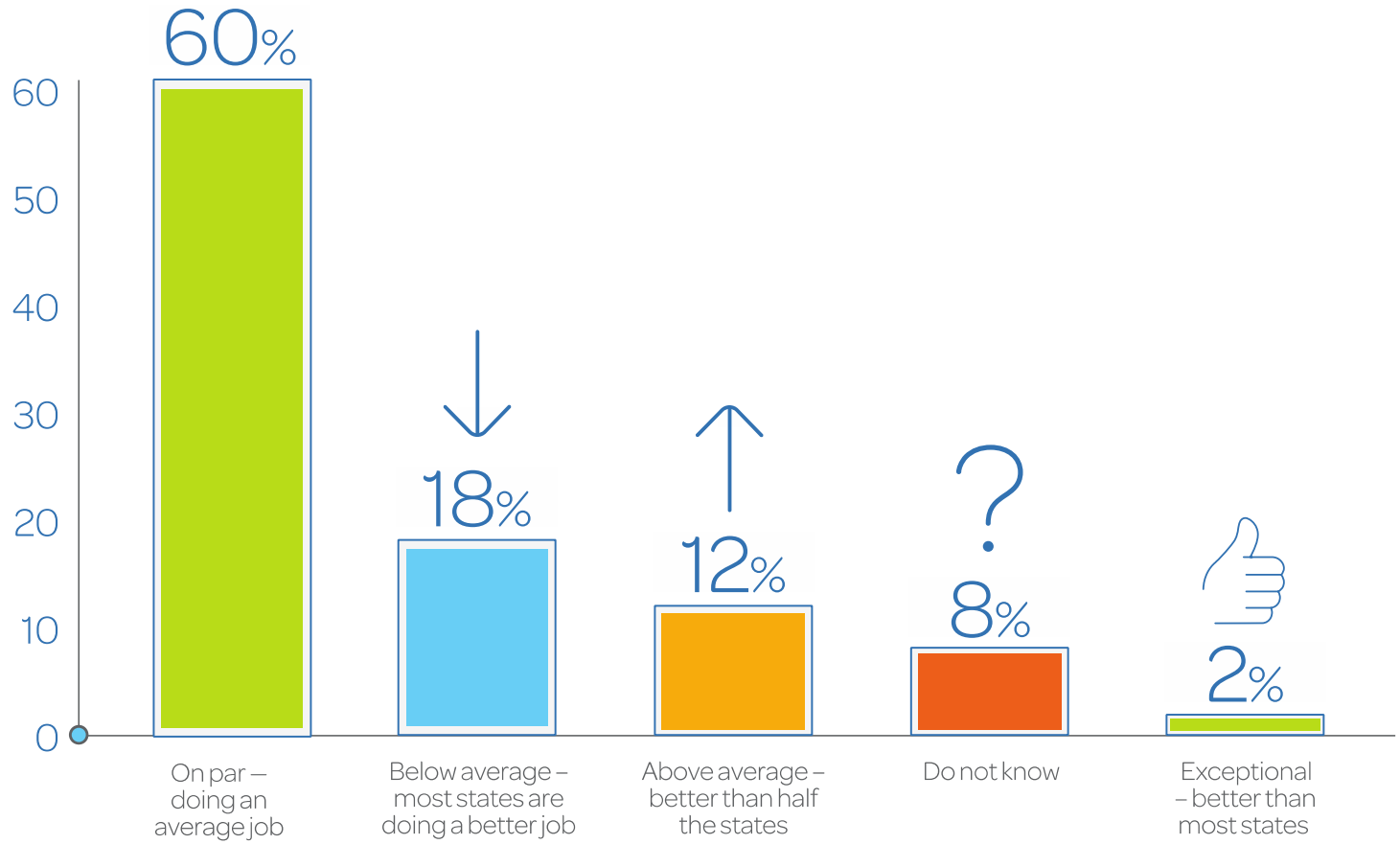
How would you rate your (your elected or appointed official's) understanding and knowledge of cybersecurity?



Rating of State's Approach to Cybersecurity

A majority of respondents reported that their state is doing an average job with its approach to cybersecurity

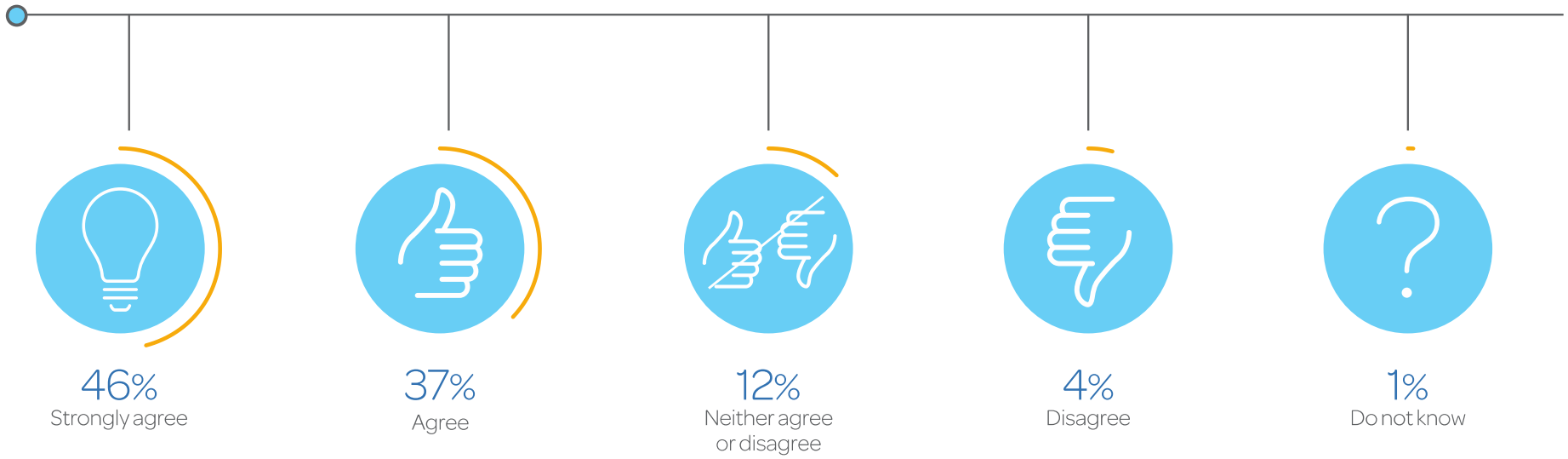
When it comes to my state's approach to cybersecurity I believe we are:



Cybersecurity as a Priority

Cybersecurity is a priority for a majority of elected and appointed officials surveyed

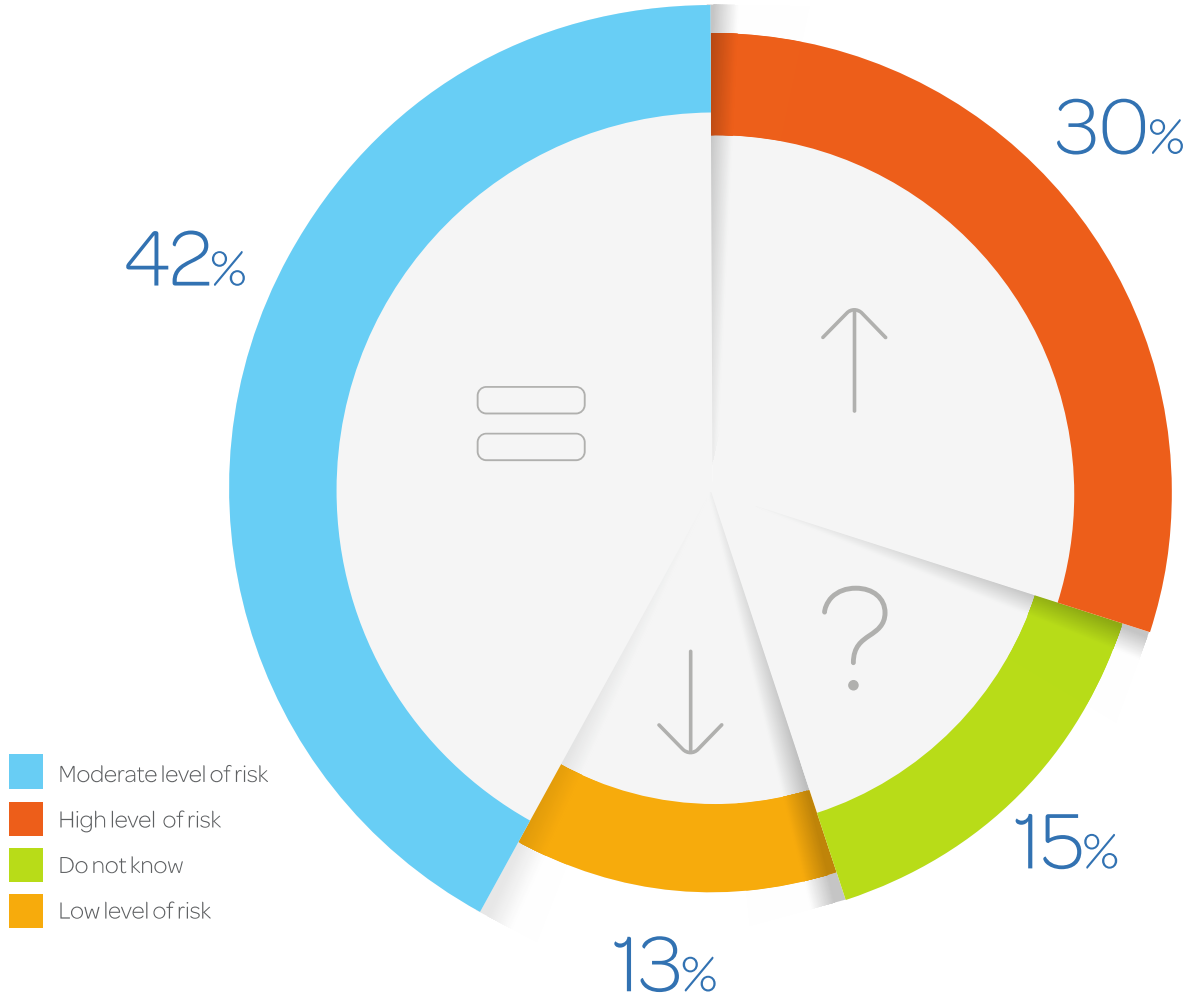
Please indicate your level of agreement with the following statement: Creating a safer, secure and trusted state network is a critical priority of mine/the state legislator or official to whom I report.



State's Current Level of Cyber Risk

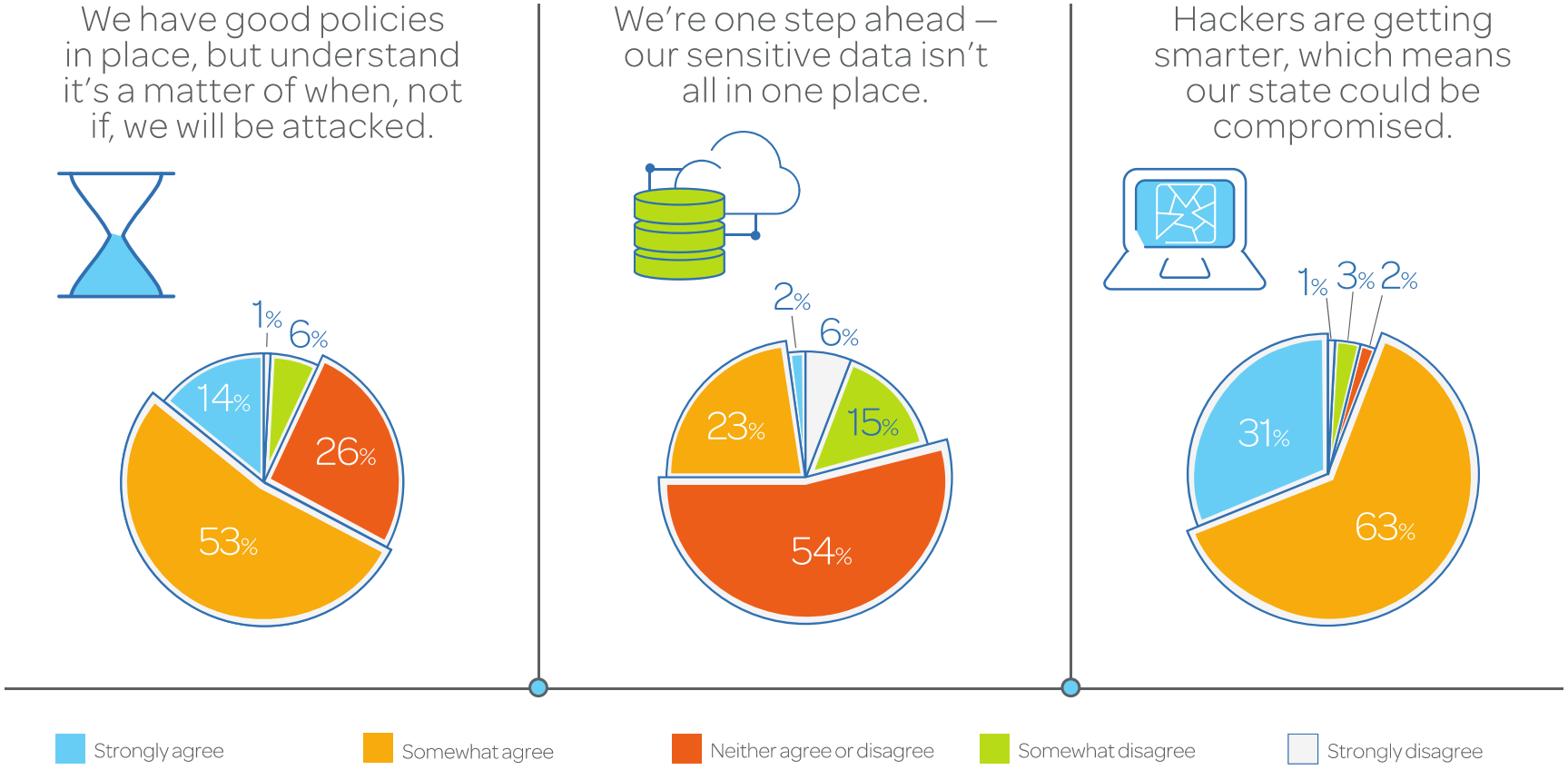
Two-thirds of respondents reported that their state's current level of cyber risk is moderate to high

I/My elected or appointed official believe/s our current level of cyber risk in the state is:



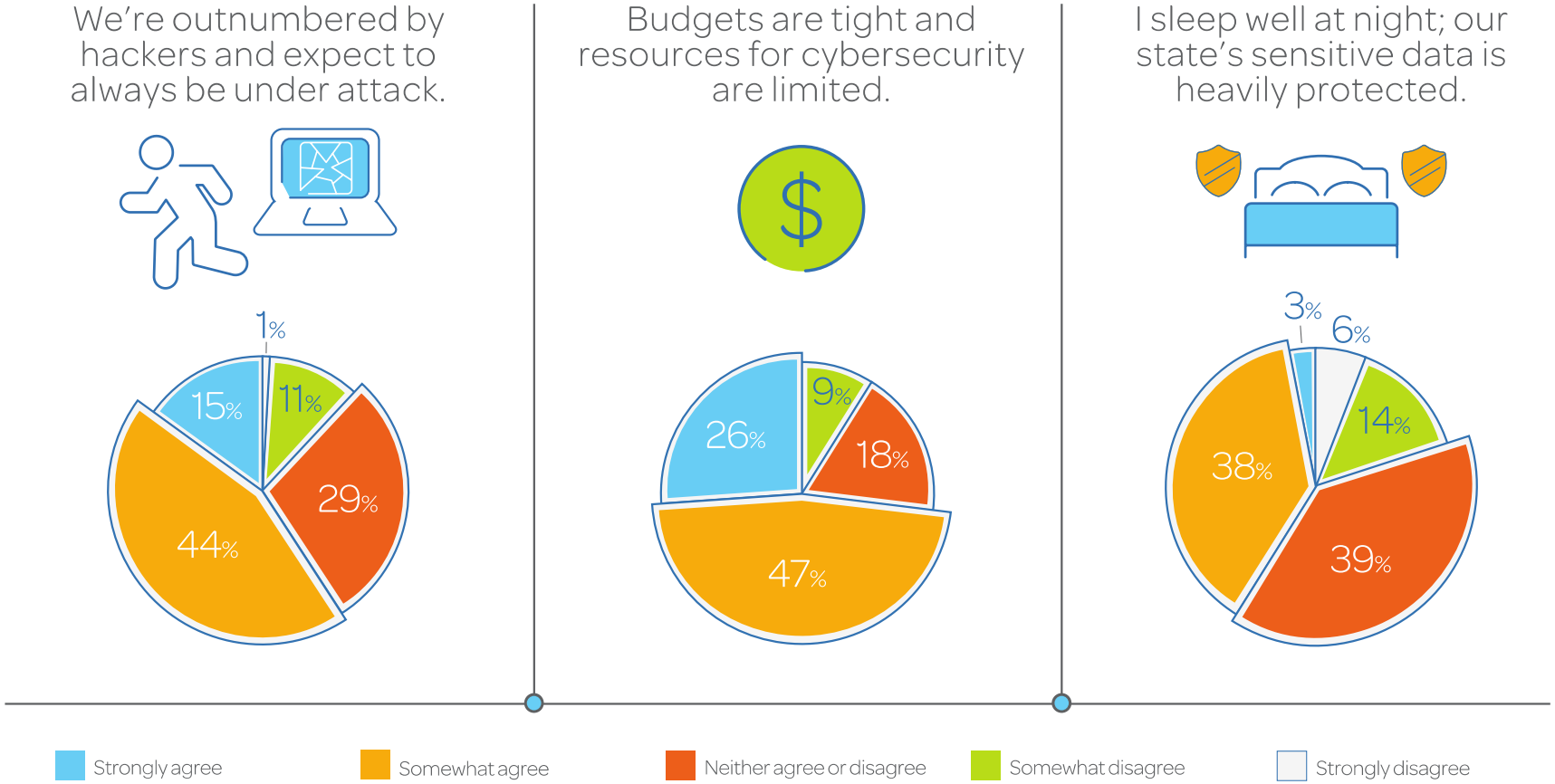
Cybersecurity Awareness

Respondents were asked to rate their level of agreement with the following cybersecurity awareness statements.



Cybersecurity Awareness

Respondents were asked to rate their level of agreement with the following cybersecurity awareness statements.



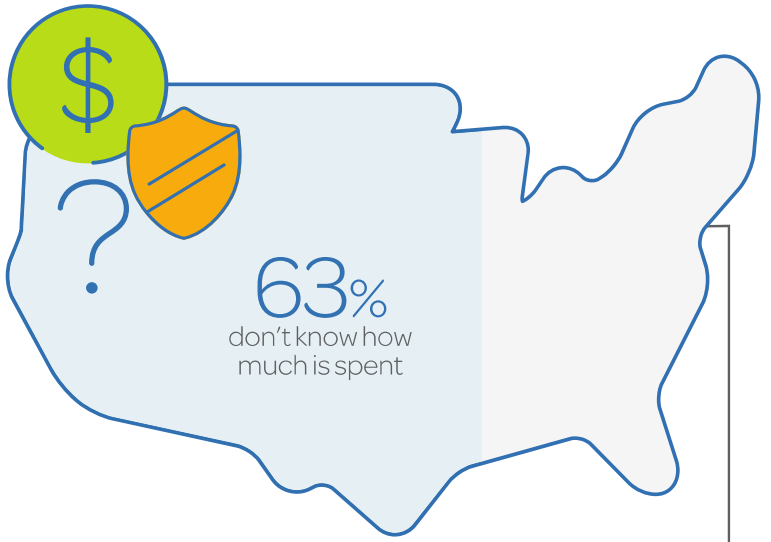
Highlights – Cybersecurity Resources

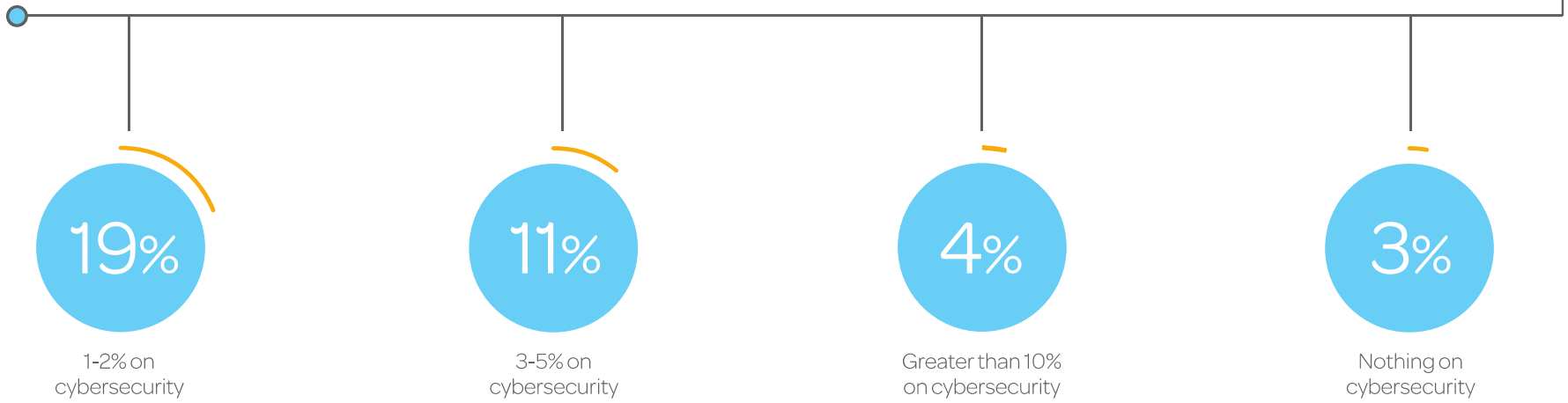
- Over half of respondents do not know how much of their state's IT budget is spent on cybersecurity
- Half of respondents acknowledge that their state has an inadequate number of cybersecurity personnel
- Respondents indicated that there is a lack of training and challenges with attracting and retaining personnel

State Cybersecurity Budget

Over half of respondents do not know how much of their state's overall information technology budget is spent on cybersecurity

What is your estimate of the overall state information technology budget that is spent on cybersecurity?

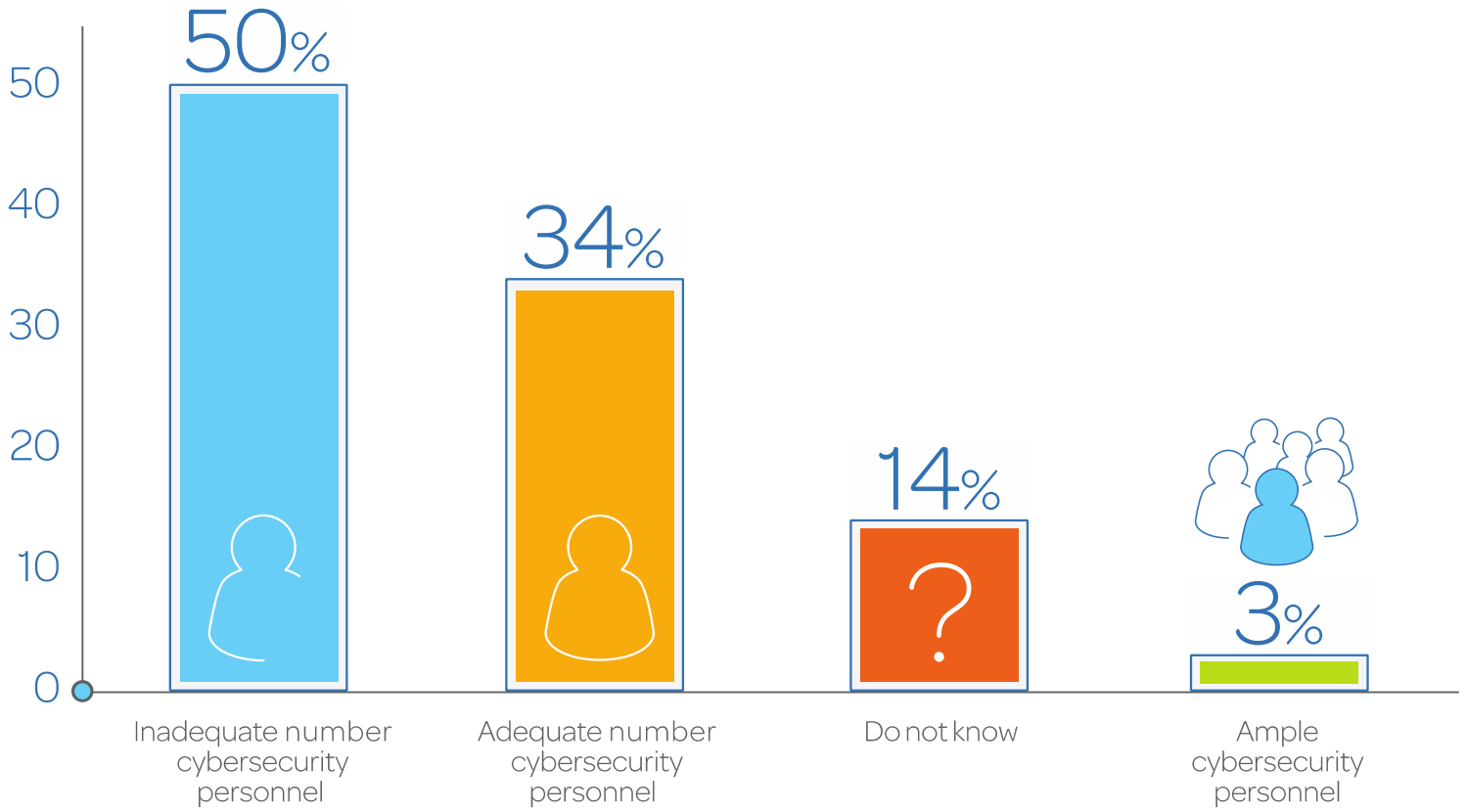




Staffing Levels for Cybersecurity Personnel

Half of respondents acknowledge that their state has an inadequate number of cybersecurity personnel

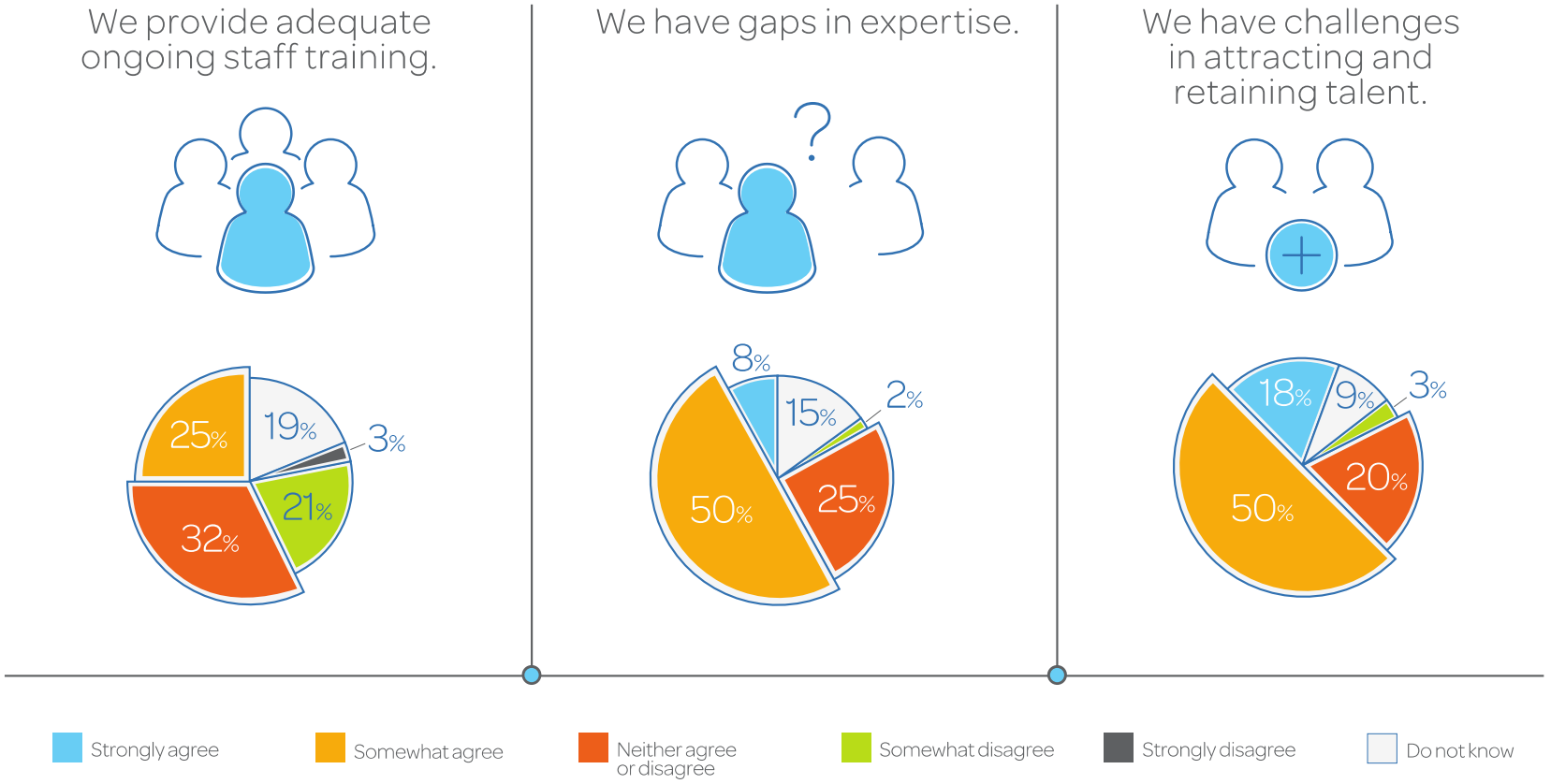
In thinking about your state's staffing levels for cybersecurity personnel, would you say that in your state you have:



Cybersecurity Staff Training and Retention

Respondents identified cybersecurity staff training and retention as challenges.

They were asked to rate their level of agreement with the following statements.



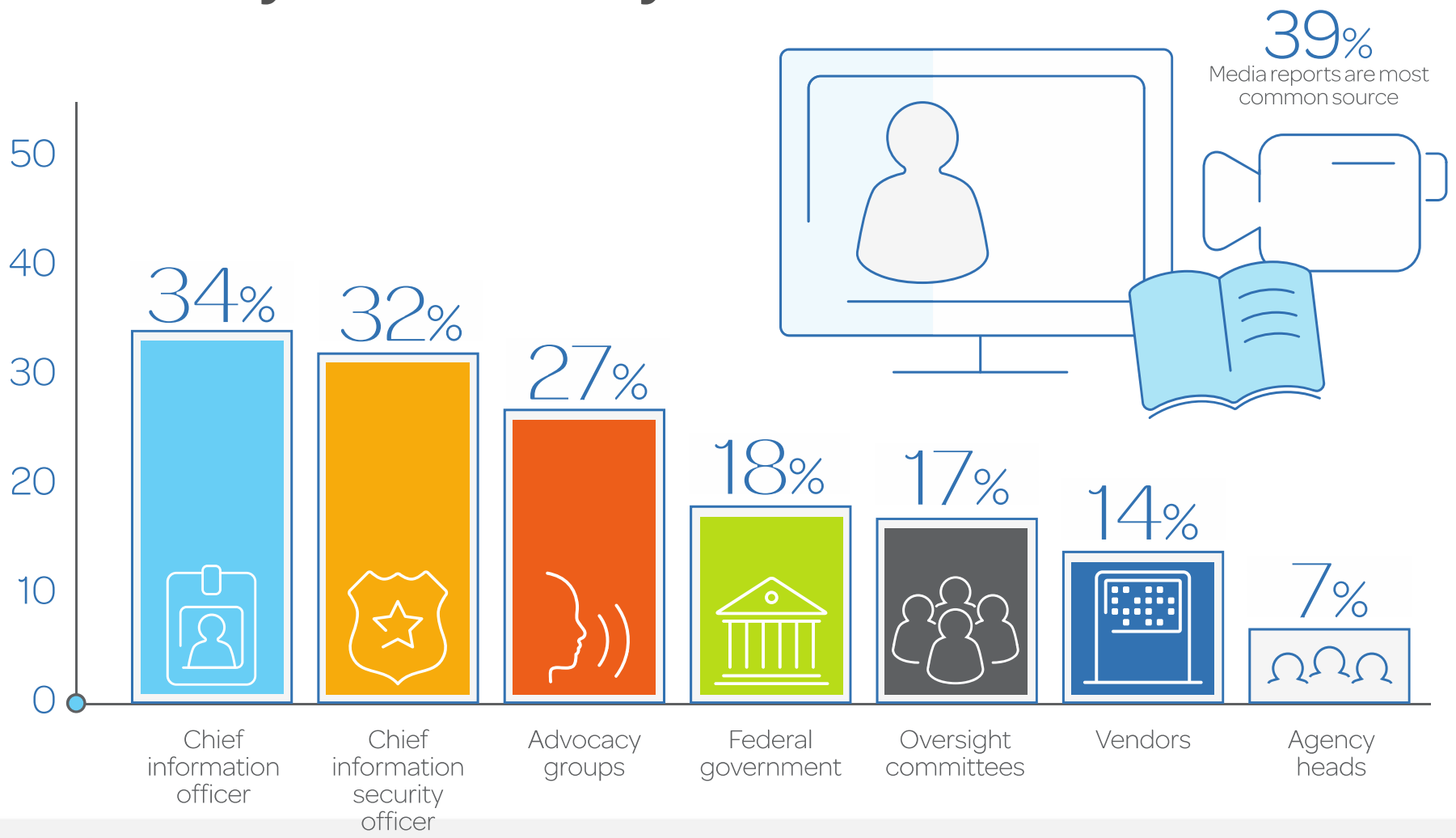
Highlights – Sources of Information

- Media reports were the most reported source for cybersecurity information
- A majority of respondents do not currently sit on a committee with a cybersecurity mandate
- A majority do not know if their state has a cyber emergency incident plan in place
- Over one-third do not know who is responsible for the development of their state's enterprise cybersecurity strategy
- Almost one-third receive security briefings on a situational basis only

Primary Sources of Cybersecurity Information

The most reported sources for cybersecurity information was media reports

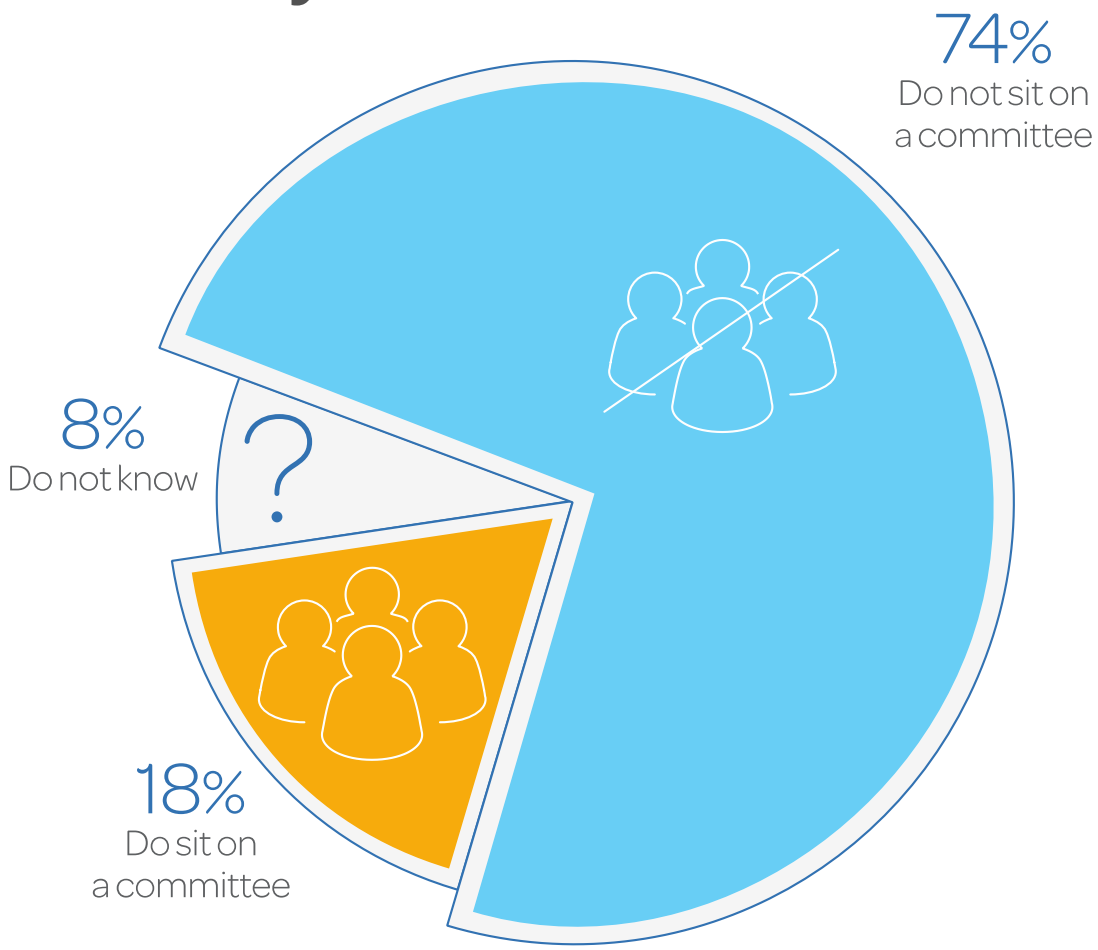
What or who are the primary sources of information about cybersecurity in your state government? Please select all that apply.



Committees with Cybersecurity Mandates

A majority of respondents are not currently sitting on a committee that has cybersecurity as part of its mandate

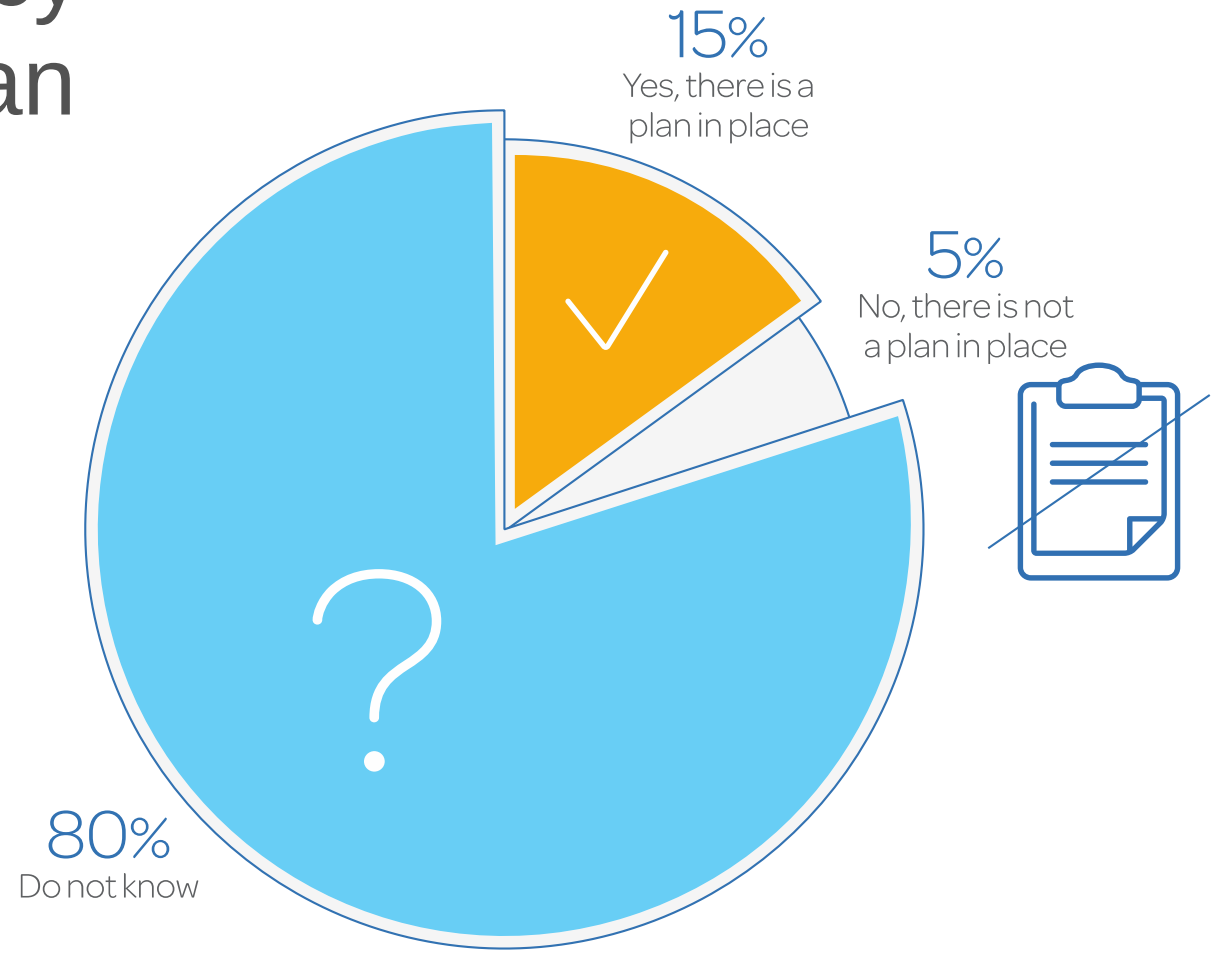
Do you (does your elected or appointed official) currently sit on a committee that has cybersecurity as part of its mandate?



State Cyber Emergency Incident Response Plan

A majority of respondents reported that they do not know if their state has a cyber emergency incident plan in place

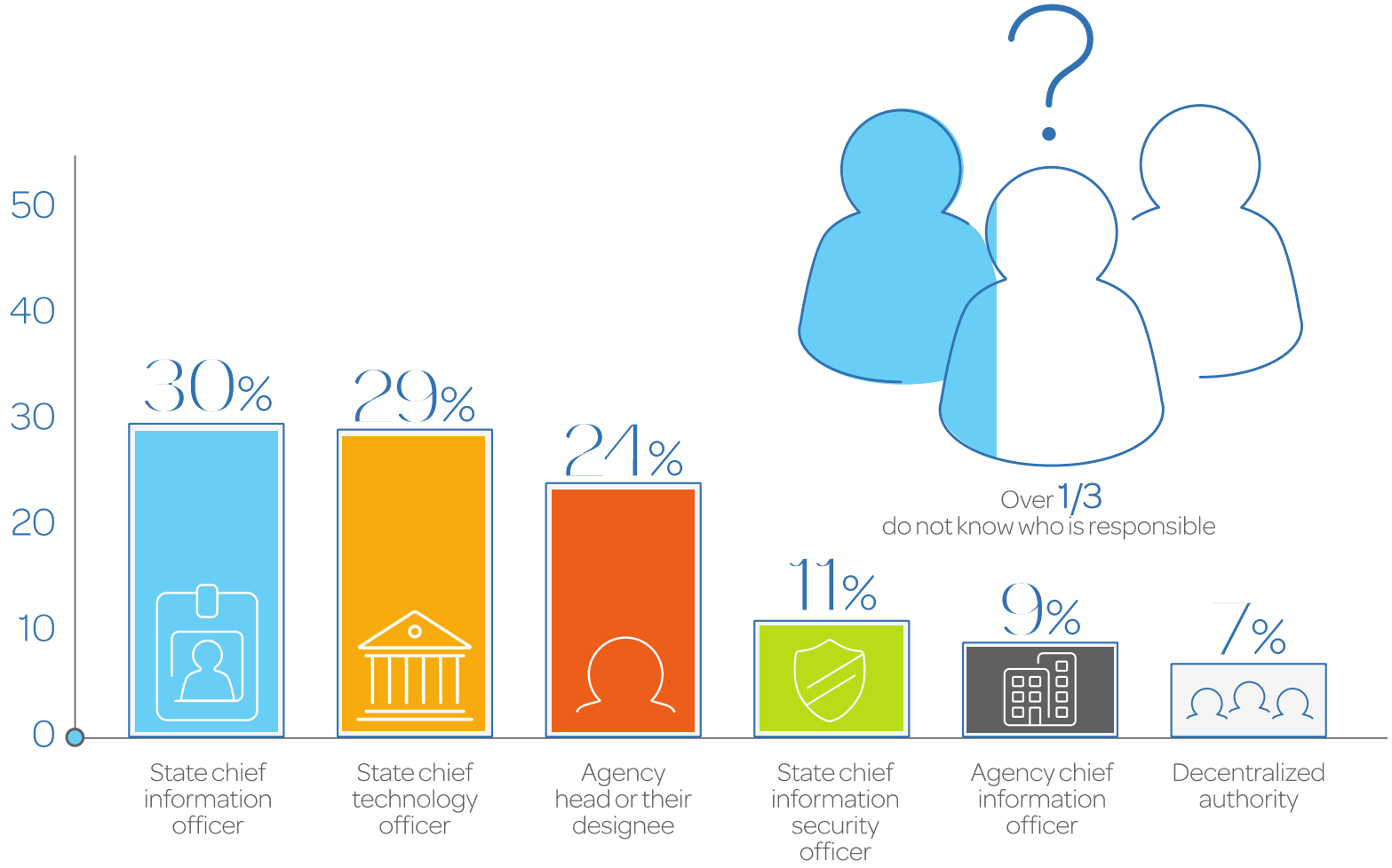
In the event of a cyber attack, we have a state cyber-emergency incident response plan in place.



Enterprise Cybersecurity Strategy Development

Over one-third of legislative officials (not staff) do not know who is responsible for the development of their state's enterprise cybersecurity strategy

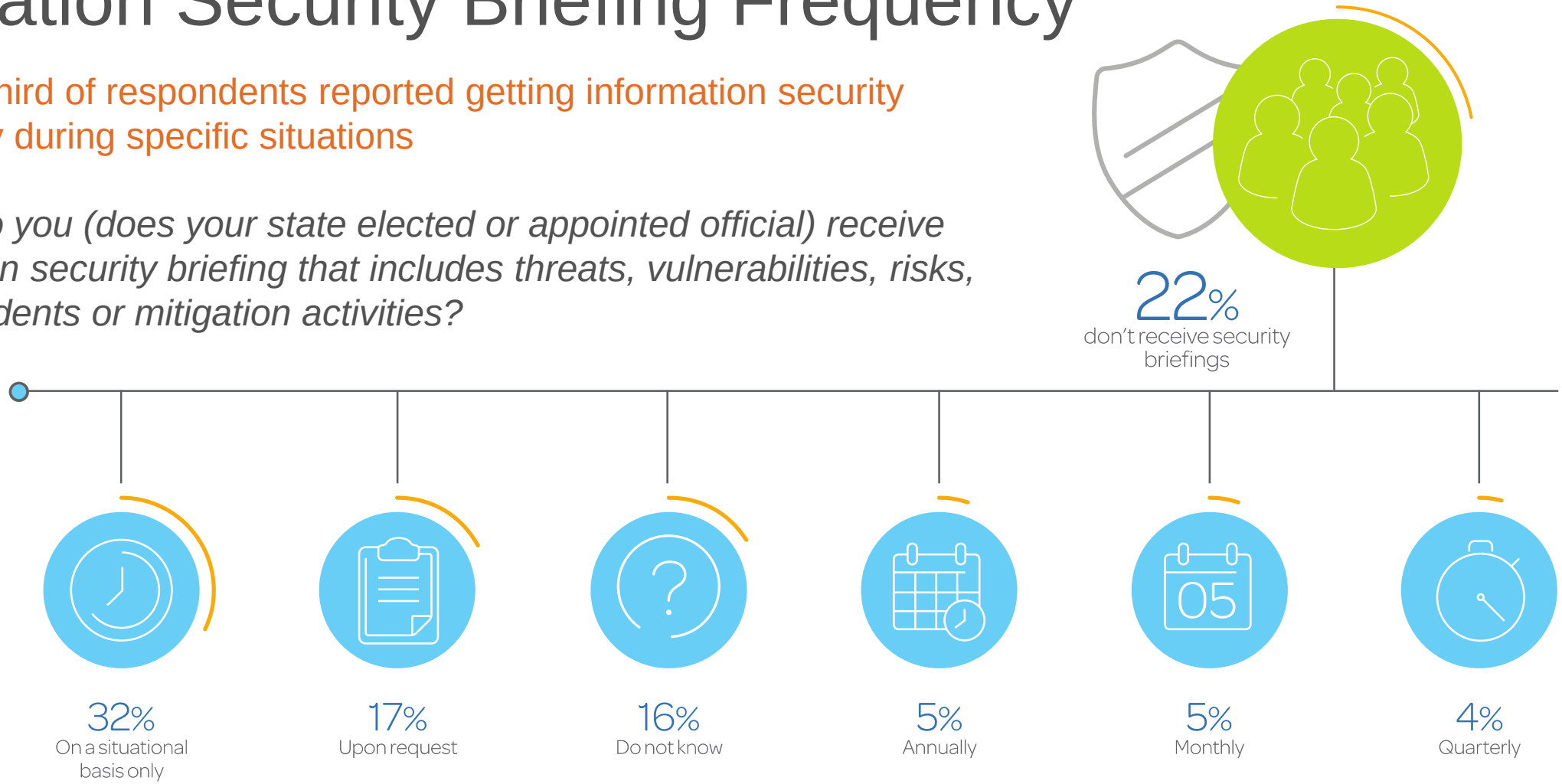
Who in your state is responsible for the development of the enterprise cybersecurity strategy, plan and controls? Please select all that apply.



Information Security Briefing Frequency

Almost one-third of respondents reported getting information security briefings only during specific situations

How often do you (does your state elected or appointed official) receive an information security briefing that includes threats, vulnerabilities, risks, controls, incidents or mitigation activities?



Highlights – Sources of Information

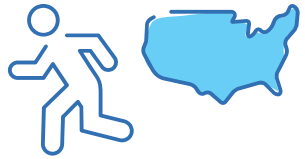
- The most reported cybersecurity threat to the state was criminal organizations outside of the U.S.
- The increasing sophistication of threats is the most reported barrier to protecting the state from cyber risks
- A majority of respondents identified interest in learning about at least one area of cybersecurity

Cybersecurity Risks to the State

A majority of respondents reported criminal organizations outside the U.S. as one of the greatest cybersecurity risks to their state

Please pick the top three cybersecurity threats that pose the greatest risk to your state.

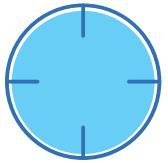
Criminal organizations outside the U.S. **70%**



Criminal organizations within the U.S. **54%**

Inside employees **39%**

Political hacktivists **54%**



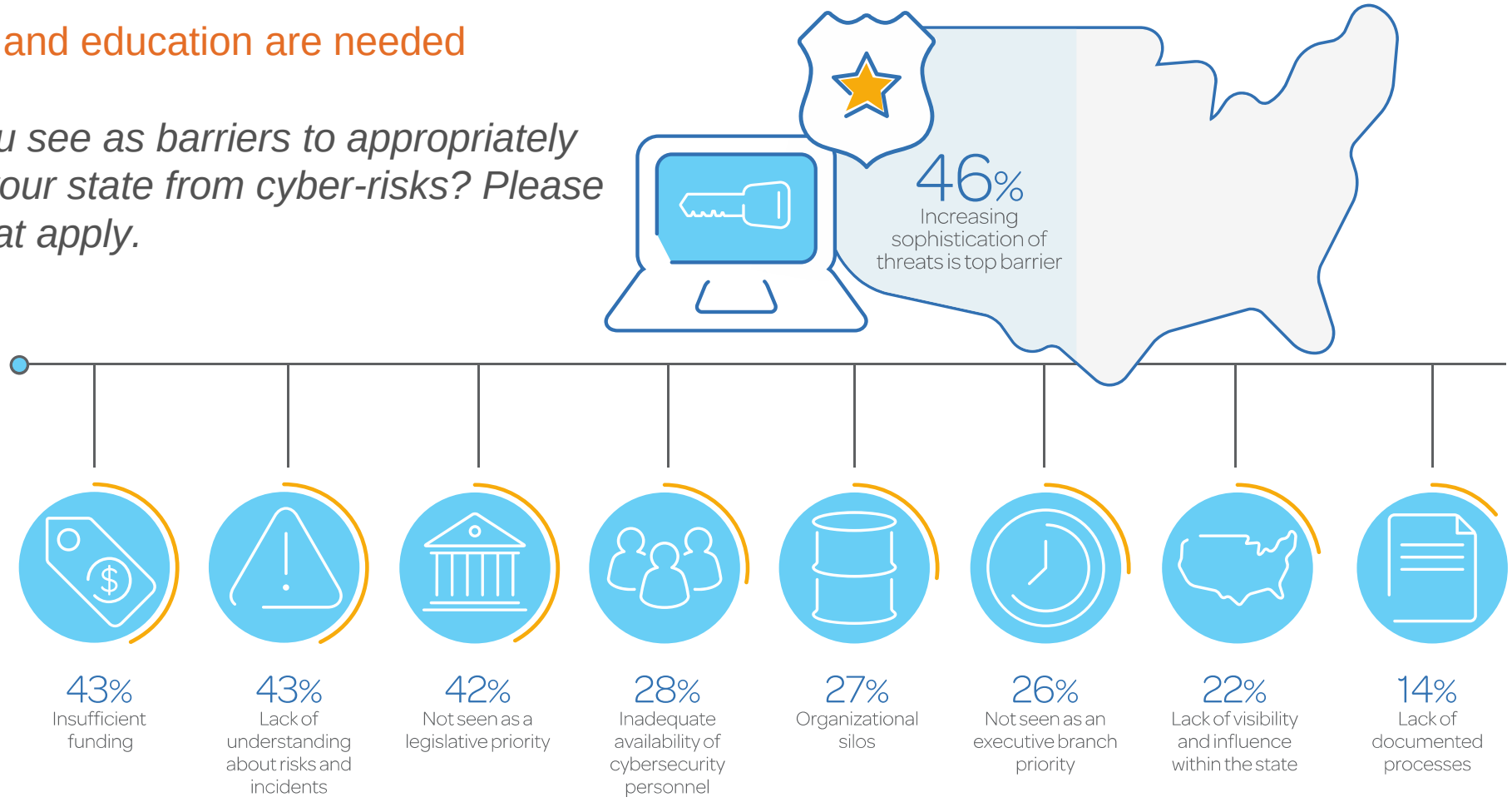
Nation states' espionage **40%**

Inside contractors **27%**

Barriers to Protecting the State from Cyber Risks

Information and education are needed

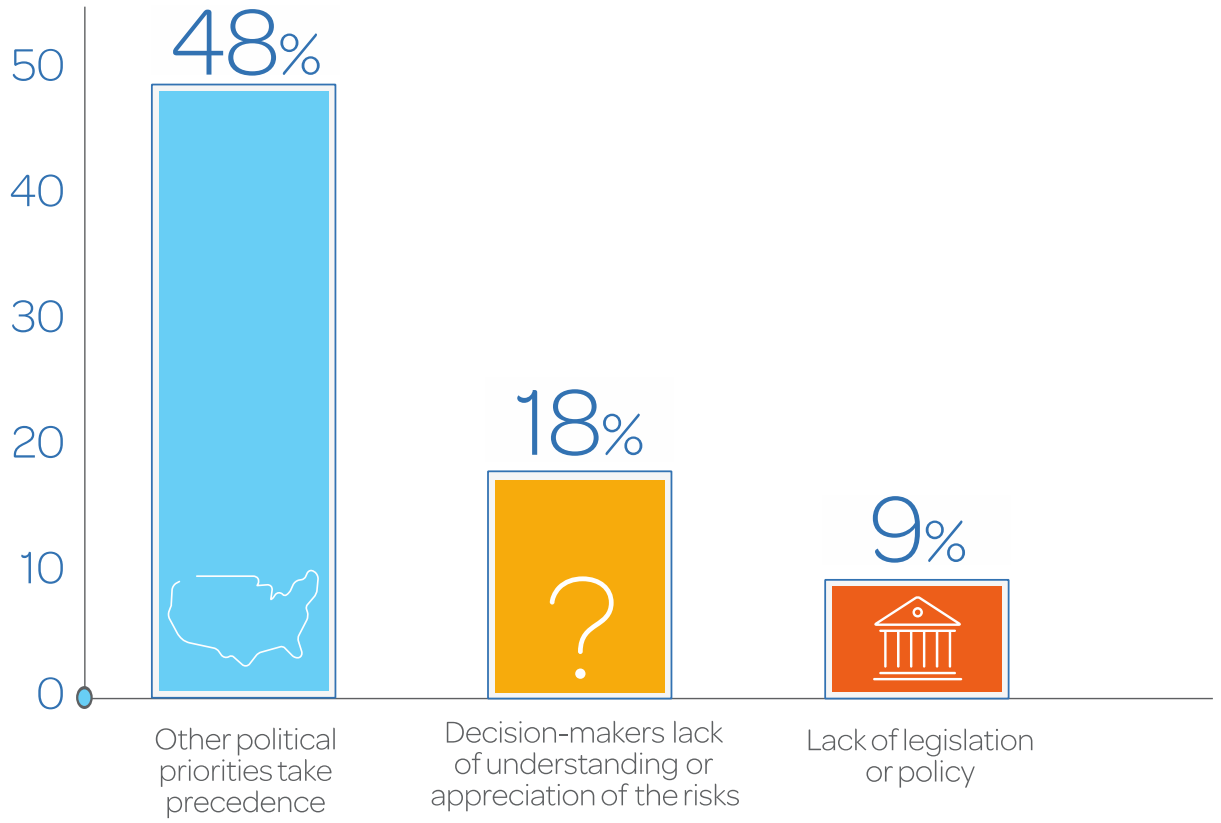
What do you see as barriers to appropriately protecting your state from cyber-risks? Please select all that apply.



Top Three Barriers to Funding Cybersecurity

Respondents who identified funding as a barrier identified factors that impede funding

If lack of sufficient funding was selected, what is keeping your state from adequately funding cyber security?

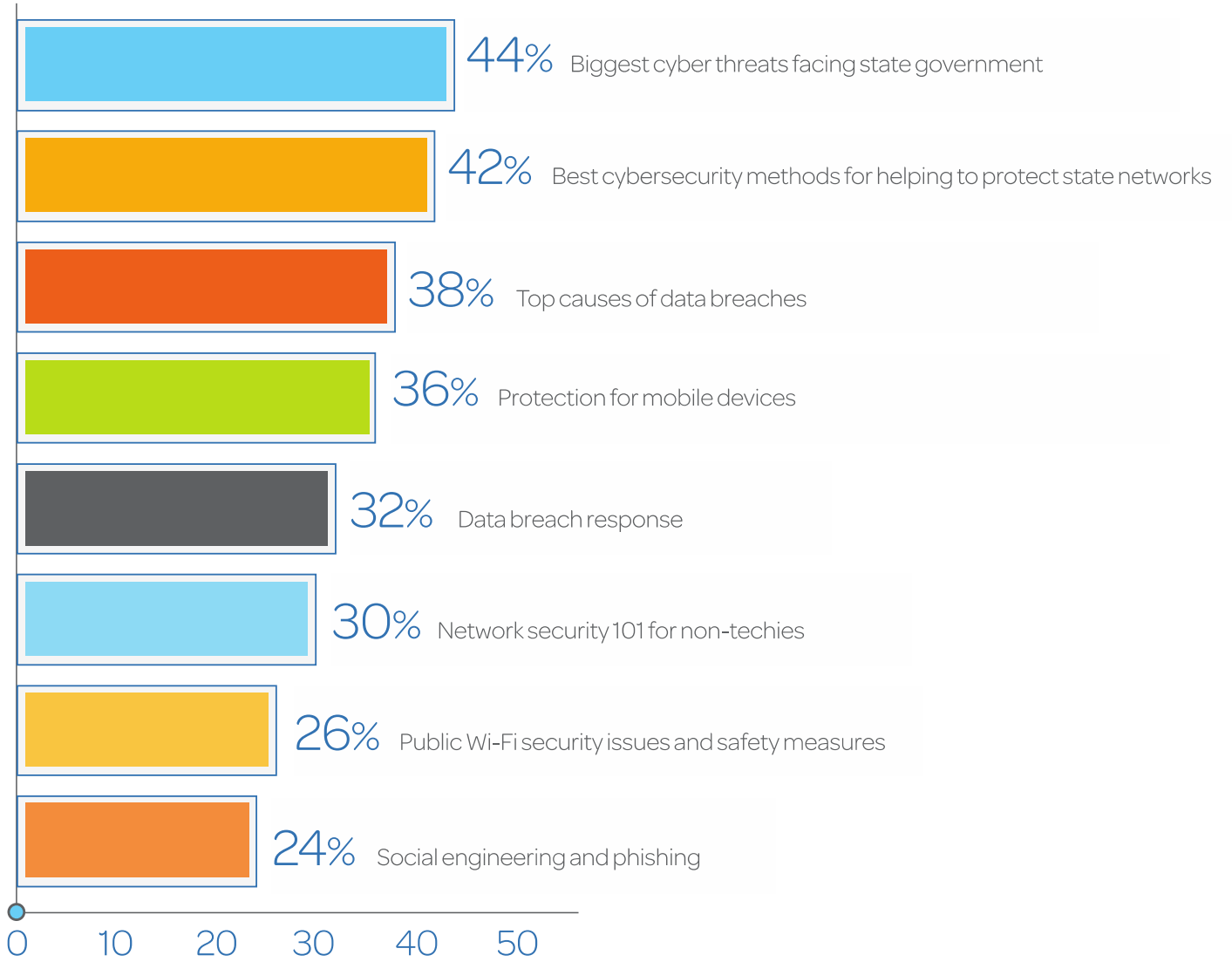


N= 44

Future Cybersecurity Education

87% of respondents identified interest in at least one area of cybersecurity

What cybersecurity topics would you (think your elected or appointed official would) like to learn more about? Please select up to five choices.



GOVERNING
INSTITUTE

The Governing Institute is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.erepublic.com / www.governing.com/gov-institute**

Thank you!

Todd Sander
Vice President, Research
e.Republic Inc.
Tsander@erepublic.com
916-932-1373